

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

ALP BAYSAL, THOMAS MAXIM and SANDRA
ITALIANO, individually and on behalf of all
others similarly situated,

Plaintiffs,

v.

OPINION AND ORDER

21-cv-394-wmc

MIDVALE INDEMNITY COMPANY and
AMERICAN FAMILY MUTUAL
INSURANCE COMPANY, S.I.,

Defendants.

In this class action, plaintiffs Alp Baysal, Thomas Maxim and Sandra Italiano, individually and on behalf of all others similarly situated, claim that defendants Midvale Indemnity Company and American Family Insurance Company, S.I., violated the Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq.* ("DPPA"). Specifically, plaintiffs claim that defendants allowed a data breach resulting in a risk of future financial harm and identity theft to themselves and putative class members. Before the court is defendants' motion to dismiss for lack of standing and failure to state a claim under Rule 12(b)(1) and (6), respectively. (Dkt. #34.) For the reasons that follow, the court will grant defendants' motion to dismiss for lack of standing.

ALLEGATIONS OF FACT

On or around May 13, 2021, the named plaintiffs each received a letter from Midvale regarding an "Unauthorized Data Disclosure." Within each letter was a notification that driver's license numbers may have been "compromised" by the

Unauthorized Data Disclosure. (Am. Compl. (dkt. #27) ¶ 25.) Generally, hackers with only basic, identifying information were allegedly able to prompt an “instant quote feature” offered by defendants to auto-fill other, personal information about that individual, including a person’s driver’s license number. (*Id.* ¶ 22.)

Plaintiffs claim defendants’ disclosure of this personal information was both negligent and a violation of the DPPA, 18 U.S.C. § 2724. As for injury, plaintiffs allege the data breach resulted in an “increased risk of fraud and identity theft.” (*Id.* ¶ 22.)

OPINION

As alluded to above, defendants seek dismissal of plaintiffs’ complaint on two bases. First, defendants contend that plaintiffs’ lack of an “injury-in-fact” denies them standing to bring these claims and this court subject-matter jurisdiction to hear their claims under Rule 12(b)(1). Second, in the alternative, defendants argue dismissal is warranted under Rule 12(b)(6) because the plaintiffs’ allegations do not state a claim upon which relief can be granted. Because the court agrees that plaintiffs lack standing, it need only reach -- and indeed must only reach -- the first challenge under Rule 12(b)(1).

To establish standing to sue under Article III of the Constitution, a plaintiff must allege an injury-in-fact traceable to the defendant’s alleged conduct. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). To meet this requirement, both the Supreme Court and Seventh Circuit Court of Appeals have recently, repeatedly emphasized that plaintiffs must allege that they suffered a concrete harm, while the allegation of a bare procedural violation, divorced from any concrete harm, does not satisfy Article III standing. *Spokeo, Inc. v Robins*, 578 U.S. 330, 340 (2016). In particular, plaintiffs must allege “that the

violation harmed or presented an appreciable risk of harm to the underlying concrete interest that Congress sought to protect by enacting the statute.” *Casillas v. Madison Ave. Assocs., Inc.*, 926 F.3d 329, 333 (7th Cir. 2019). In other words, a plaintiff must be concretely harmed by a defendant’s statutory violation to satisfy Article III standing. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2205 (2021).

Here, defendants contend plaintiffs fail to allege any concrete injury; rather, they argue plaintiffs allege injuries too speculative to confer standing. (Defs.’ Opening Br. (dkt. #30) 10.) Specifically, defendants argue that in order for the injury of future harm to satisfy the standing requirements in a data-breach case like this one, the data at issue needs to be highly sensitive such as “social security numbers or payment card information.” (*Id.* at 12.) More specifically, where plaintiffs claim a risk of *future* harm by virtue of a data breach -- whether identity theft or fraud -- the Seventh Circuit requires that there must be an “‘objectively reasonable likelihood’ that an injury will occur.” *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 410 (2013)).

In *Remijas*, the Seventh Circuit found that plaintiffs had alleged a substantial and plausible risk of identity theft and fraudulent purchases on their credit cards. 794 F.3d at 688. Similarly, in *Lewart v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), the plaintiffs had their credit and debit card data stolen, and a named plaintiff experienced actual fraudulent charges as a result. As such, the Seventh Circuit found an actionable risk present and imminent for the other named plaintiffs as well, thus satisfying the standing requirement under Article III. *Id.* at 967. In contrast, defendants contend that plaintiffs

have failed to allege any concrete injury: unlike in *Remijas*, here, neither the data allegedly stolen could be reasonably inferred to create an impending risk of financial harm, nor do plaintiffs allege actual harm to one of the plaintiffs as in *Lewart*; thereby distinguishing risk of possible access to driver's license numbers from proven access to credit card numbers at stake in *Remijas* and *Lewart*. (Defs.' Br. (dkt. #30) 10.)

In response, plaintiffs offer several responses; however, none of which have much traction. *First*, plaintiffs repeat that defendants' failure to protect their personal information resulted in a risk of future identity theft and harm, pointing to a list of harms alleged in their complaint that *could* happen when driver's license information is disclosed, including having that information sold on the dark web, the creation of synthetic identities and the ability to access more personal information. (Am. Compl. (dkt. #27) ¶¶ 13-17.) Fortunately for plaintiffs, all of these injuries are speculative, things that could happen but have not happened. In *Ewing v. MED-1 Solutions, LLC*, 24 F.4th 1146 (7th Cir. 2022), the Seventh Circuit underscored the holding in *TransUnion* that a risk of future harm is not sufficient to satisfy standing without more. *Id.* at 1152.

While plaintiffs contend each of these harms are imminent, Seventh Circuit case law has held that the imminency of a harm in data breach cases depends on the type of information disclosed in the breach, if not proof of some actual injury. *E.g.*, *Remijas*, 794 F.3d at 688; *Lewart*, 819 F.3d at 963. Thus, while those decisions both bound the risk of harm that can be done when information like credit card and social security numbers are disclosed sufficiently imminent to confer standing, other courts have similarly distinguished the disclosure of driver's license numbers from credit card information,

concluding that the risks associated with the former are not sufficiently imminent to satisfy Article III standing. *E.g., Antman v. Uber Techs.*, No. 3:15-CV-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 18, 2015) (finding that the theft of names and driver's license numbers did not create sufficient injury-in-fact to satisfy Article III). Similarly, the court is compelled to find that the risk of harm posed by the disclosure of driver's license numbers is not imminent and too speculative to satisfy Article III standing.

Second, plaintiffs contend that the loss of time and expense that must now be incurred to monitor their credit reports for the threat of future harm by virtue of defendants' possible release of their driver's license numbers constitutes a distinct injury sufficient to establish standing. However, plaintiffs' argument only has traction where there is an objectively reasonable risk of harm. As plaintiffs themselves acknowledge in their responsive brief, the Seventh Circuit recognizes "standing through lost time if there is a future risk of harm based on a hacker's ability to access the compromised information and commit identity theft or fraud." (Pls.' Opp'n (dkt. #33) 9 (citing *Lewart*, 819 F.3d at 965, 967; *Remijas*, 794 F.3d at 693).) Once again, therefore, plaintiffs are left to speculate as to a potential harm that could occur due to the disclosure of their driver's license information, rather than allege an actual harm.

As already explained, the threat of future, speculative harm cannot satisfy Article III standing without more. *Transunion*, 141 S. Ct. 2190. This "more" in data breach cases, according to Seventh Circuit case law, is the imminency of the harm -- whether alleged by the obviousness of misuse of credit card information or by concrete examples of some plaintiffs suffering a concrete harm from the data breach. *Lewart*, 819 F.3d at 965, 967;

Remijas, 794 F.3d at 693. Regardless, because the specific information disclosed in the data breach here does not obviously rise to the level that the Seventh Circuit has deemed will result in imminent harm, the court must also find that any alleged loss of time and expense tied to these speculative harms is not sufficient proof of an injury-in-fact to satisfy Article III.

Third, in their amended complaint, plaintiffs attempt to strengthen the allegations as to standing by alleging specific instances of identity theft. In particular, plaintiff Maxim now alleges receiving notice from Charles Schwab informing him that a brokerage account was fraudulently opened in his name, and he discovered an unauthorized purchase on his credit report using Klarna software.¹ (Am. Compl. (dkt. #27) ¶ 23.) However, plaintiffs stop short of alleging in good faith that these instances of attempted identity theft are somehow traceable back to the disclosure of plaintiffs' driver's license numbers, and for good reason. In their brief, defendants contend that the alleged injuries cannot have occurred where the data breach compromised access to driver's license numbers alone, as both of the alleged injuries would require a social security number or other information unrelated to a driver's license number. (Defs.' Br. (dkt. #30) 11-12.) Plaintiffs do not dispute this, and the court agrees with defendants that a driver's license number alone was unlikely to be the sole piece of information used to open these two accounts without plaintiff Maxim's permission. As such, plaintiffs have again failed to plausibly allege that

¹ "Klarna Bank AB, commonly referred to as Klarna, is a Swedish fintech company that provides online financial services such as payments for online storefronts and direct payments along with post-purchase payments." "Klarna," Wikipedia, <https://en.wikipedia.org/wiki/Klarna>.

Maxim’s instances of identity theft can be traced to the disclosure at issue here.²

Fourth, and finally, plaintiffs allege that disclosure of their personal information resulted in anxiety and emotional distress. Unfortunately for plaintiffs, this argument does not even leave the gate. The Seventh Circuit explicitly held these alleged injuries are *not* sufficiently concrete to confer standing. *Wadsworth v. Kross, Lieberman & Stone, Inc.*, 12 F.4th 665, 668 (7th Cir. 2021) (abstract harms like “stress,” “anxiety,” and “uncertainty” are not bases for FDCPA standing). In *Wadsworth* in particular, the plaintiff alleged that she suffered emotional harms, including personal humiliation, embarrassment, loss of sleep, and constant worrying. Nevertheless, the court found these emotional harms, without some additional concrete injury to the plaintiff, do not satisfy the injury-in-fact requirement for Article III standing, in part because such litigation would become too prevalent. *Id.* at 668-69 (“These are quintessential abstract harms that are beyond our power to remedy. The same is true of the stress and embarrassment that Wadsworth complains of in this case.”).

The same applies to plaintiffs in this case: they claim the possible disclosure of their driver’s license numbers resulted in a loss of privacy, anxiety, and emotional distress. However, plaintiffs have failed to plead a concrete, non-emotional harm, along with these

² Plaintiffs also contend they were harmed because the disclosure of their driver’s license information resulted in unemployment insurance benefits fraud. Even if this were true, plaintiffs do not allege a harm to them, but rather a harm to the state. This does not satisfy Article III’s “injury in fact” requirement. *See Campbell v. Gaither*, No. 3:11-cv-190-FDW, 2011 WL 1838779, at *3 (W.D.N.C May 13, 2011). In so holding, the court does not mean to suggest that access to confidential driver’s license numbers could *not* cause sufficient injury to satisfy Article III standing, but only that without allegations of specific, concrete examples of causal injury or of rampant fraud more generally using this data, as in the case of stolen credit card information, plaintiffs have failed to make that showing.

emotional harms, that resulted from the disclosure of their driver's license information.

Having failed to allege an injury-in-fact in their original complaint nor in their amended complaint, the court has no choice but to dismiss both their state and federal claims for lack of subject matter jurisdiction.

ORDER

IT IS ORDERED that defendants' motion to dismiss for lack of standing (dkt. #30) is GRANTED, and plaintiff's amended complaint is DISMISSED WITHOUT PREJUDICE.

Entered this 19th day of April, 2022.

BY THE COURT:

/s/

WILLIAM M. CONLEY
District Judge